## *Emergency Telephone Numbers*

---

In the Forrestal, Germantown, Cloverleaf, and 955 L'Enfant buildings,

**dial extension 166 for emergencies**

In the 270 Corporate and 950 L'Enfant buildings,

**dial 9-911**

---

**Non-Emergency Numbers:**

Germantown, Cloverleaf, and the 270 Corporate Center dial: **3-2403**; Forrestal dial: **6-6900**; 950 L'Enfant Plaza dial: **202-863-7901**; and 955 L'Enfant Plaza dial: **6-9384**

United States Department of Energy

**Office of Headquarters Security Operations**
**Headquarters Technical and Information Security Team (HS-1.31)**

*For assistance contact: 301-903-9990*

# U. S. Department of Energy

# HEADQUARTERS SECURITY OVERVIEW HANDBOOK

**February 2007 Edition**

*Produced by:*
Office of Headquarters Security Operations

Headquarters Technical and Information Security Team (HS-1.31)
301-903-9990

# HEADQUARTERS SECURITY OVERVIEW HANDBOOK

**February 2007**

penalty (fine) not to exceed $100,000 per offense. In publishing 10 CFR Part 824, DOE has determined that civil penalties under Part 824 will only be assessed for violations of requirements for the protection of classified information (Restricted Data, Formerly Restricted Data and National Security Information) in particular violations of classified information security requirements published in DOE Security Directives (DOE Manuals 470.4-1 through 6). Civil penalties for failure to protect classified information will not be assessed against individual employees, but will only be assessed against a company that has entered into a contract or agreement with DOE.

## A Final Word

Security is everyone's responsibility. Just as a chain is only as strong as its weakest link, the Headquarters security program is subject to the strengths and weaknesses of our employees and contractors. Regardless of your status (DOE employee, consultant, contractor, subcontractor, or individual permitted to access DOE facilities), DOE needs you and your dedication to ensure the success of its security program.

**LEGAL AND ADMINISTRATIVE**
Administrative and legal sanctions may be imposed on individuals who knowingly or willfully disregard security procedures and/or Federal regulations. Such administrative and legal sanctions include, but are not limited to, the following:

- **Administrative Sanctions** may include reprimand, suspension, reassignment, termination of classification authority, loss or denial of access authorization, termination of employment, or other sanctions in accordance with applicable laws and agency regulations.

- **Legal Sanctions**

– Title 18, U.S.C., section 793. Gathering, transmitting, or losing defense information.
– Title 18, U.S.C., Section 794. Gathering or delivering defense information to aid foreign government.
– Title 18, U.S.C., Section 798. Disclosure of classified information.
– Title 18, U.S.C., Section 1924. Unauthorized removal and retention of classified documents or material.
– Atomic Energy Act of 1954, section 224. Unauthorized Communication of Restricted Data.

An individual who has been found guilty of one or more of these felonies may be sentenced to pay a fine of not more than $250,000 and/or may be imprisoned for any term of years or for life, or may be punished by death.

**SECURITY ENFORCEMENT PROGRAM**
The Security Enforcement Program is designed to implement the requirements of Title 10, Code of Federal Regulations, Part 824. This rule was published by DOE to implement Section 234B of the Atomic Energy Act of 1954. Section 234B stipulates that a contractor or subcontractor to the DOE who violates any rule, regulation, or order relating to the safeguarding or security of Restricted Data, other classified information, or sensitive information shall be subject to a civil



# Table of Contents

# MAKING A DIFFERENCE

The Department of Energy (DOE) is responsible for some of the nation's most sensitive programs. These programs are critical to our country's economic well being and national defense. Protecting the national security of the United States is an integral requirement of our mission at DOE. Critical to this requirement is the protection of classified matter and unclassified controlled information. Both Federal and contractor employees must demonstrate sound security practices every day and management must create and foster a work environment that allows free and open expression of security concerns and timely corrective action. As such, security at DOE Headquarters depends on the vigilance of everyone – from senior managers to individual employees.

# INTRODUCTION

Protecting the national security of the United States is an integral requirement of the mission of the DOE. Critical to this requirement is the protection of classified and unclassified controlled information. Accordingly, this information requires special protection requirements. These requirements are established in various DOE security directives, Executive Orders and Federal Laws. This Headquarters Security Overview Handbook provides a general reference for conducting some of your security responsibilities. However, by no means does it describe the total extent of your obligations to identify and protect classified and unclassified controlled information. Your knowledge of the Department's security policies and procedures is only the first step in the continuing process of security awareness. Please take time to read and become familiar with the contents of this Handbook.

An additional resource for more in-depth understanding of your security responsibilities is the Headquarters Facilities Master Security Plan (HQFMSP). This Plan is a comprehensive security plan that implements Departmental security policy for all Headquarters organizations. This plan is available to you through your Element's Headquarters Security Officer (HSO).



**Reporting Requirements**

| WHO | WHAT | WHEN | WHERE |
|---|---|---|---|
| Contractor supervisor | Contractor access authorization applicant declines employment offer or fails to report to duty | Verbal notification within 2 days/ Written notification within 10 days after verbal notification | Office of Personnel Security |
| | An event for which a contractor's access authorization is terminated, or access to classified matter or SNM is restricted or withdrawn by the contractor | Verbal notification within 2 days/ Written notification within 10 days after verbal notification | Office of Personnel Security |
| | Contractor access authorization applicant or holder is hospitalized or treated for mental illness or other condition that may affect judgment or reliability | Immediate | Office of Personnel Security |
| | Contractor access authorization applicant or holder is subject of information of personnel security interest or, if a foreign national, changes in citizenship status | Verbal notification within 2 days/ Written notification within 10 days after verbal notification | Office of Personnel Security |

**Note: Consult the Headquarters Facilities Master Security Plan or your HSO to obtain a copy of the Sensitive Countries List or Sensitive Subject List.**

**Reporting Requirements**

| WHO | WHAT | WHEN | WHERE |
|---|---|---|---|
| Access Authorization applicants and holders | Approaches or contacts by anyone attempting to obtain unauthorized access to classified information or SNM | Immediate | Office of Headquarters Security Operations, or if outside US, US Embassy or Consulate |
| Access Authorization holders | Violations of security regulations | Immediate | Office of Headquarters Security Operations, HSO or Contractor Security Office |
| | Any contact with a known or suspected intelligence officer from another country | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| All supervisors | DOE or contractor access authorization holder hospitalized for mental illness or treated for any condition that may cause a significant defect in judgment or reliability | Verbal notification within 8 hours/ Written notification within 10 days after the verbal notification | Office of Personnel Security |
| | An access authorization is terminated or should be terminated | Verbal notification within 2 days/ Written notification within 10 days after verbal notification | Office of Personnel Security |



# RESPONSIBILITIES

As a Federal or contractor employee of DOE, you are personally responsible for the proper use, handling, storage and protection of classified matter in your care. Other Headquarters Offices also have a role in assisting you in your security responsibilities.

HSS
Office of Health, Safety and Security

# OFFICE OF SECURITY OPERATIONS

The Office of Security Operations' mission is to establish and implement a comprehensive and efficient security program to protect the DOE Headquarters facilities, personnel and classified and unclassified controlled information. This Office's responsibilities include:

- Managing the Headquarters Security Officer (HSO) program.
- Assisting the Headquarters Program Offices and Staff Offices in discharging their security responsibilities.
- Developing Headquarters-specific implementation guidance in response to Departmental safeguards and security directives. Implementation guidance is contained in the Headquarters Facilities Master Security Plan (HQFMSP).
- Managing the Personnel Security Program for Headquarters.
- Managing the Headquarters Technical & Information Security Team.
- Managing the Headquarters Physical Protection Team.
- Coordinating with other Government agencies on security issues and security operations.

# HEADQUARTERS SECURITY OFFICERS (HSOs)

Each Headquarters organization has designated HSOs who are the security representatives for their organizations. HSOs are responsible for all security-related activities within their organization and are conduits for the timely dissemination of security information throughout their organization. HSOs participate in the HSO program that is managed and directed by the Office of Security Operations.

# THE COUNTERINTELLIGENCE DIRECTORATE

The Counterintelligence Directorate conducts counterintelligence activities to protect DOE/NNSA classified and sensitive programs and information, personnel, and assets from foreign intelligence collection and international terrorist activities; and to detect and deter trusted insiders who would engage in activities on behalf of a foreign intelligence service or foreign terrorist entity.

Counterintelligence (CI) is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities.

**Facts about counterintelligence:**

- Foreign intelligence services and international terrorist organizations still gather information.
- DOE employees, information and facilities are potential targets.
- Foreign intelligence services foster professional and personal relationships to elicit desired information.



**Reporting Requirements**

| WHO | WHAT | WHEN | WHERE |
|---|---|---|---|
| Access Authorization Applicants and holders<br><br>Note: Contractor supervisors are required to report when aware of these and other events which may impact a Subordinate's access authorization | Events which may impact your access authorization:<br>• Arrest, charge, detention (but not traffic offense fined $250 or less<br>• Filing for Bankruptcy<br>• Garnishment of Wages<br>• Legal name Change<br>• Change in Citizenship<br>• Employment or association with foreign or foreign-owned business<br>• Hospitalization for mental illness; treatment for drug/alcohol abuse<br>• Marriage or cohabitation | Verbal Notification within 2 days and Written Notification within 3 days after the verbal notification<br><br>45 days after union began | Office of Personnel Security<br><br>Office of Personnel Security |

## Reporting Requirements

| WHO | WHAT | WHEN | WHERE |
|---|---|---|---|
| | Unauthorized access is sought to classified or unclassified controlled information | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| | Espionage information; e.g., belief you may be target of an attempted exploitation by a foreign entity | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| | All substantive contacts or relationships with citizens of sensitive countries | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| | Official travel to a sensitive country, or to a non-sensitive country if it involves a sensitive subject | 45+ days prior to departure & upon return | Foreign Travel Management System or WRCO |
| | Official travel to a non-sensitive country | 30+ days prior to departure | Foreign Travel Management System |
| All Contractor employees | All foreign travel done with foreign monetary support | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| All DOE Federal employees | All foreign travel done with substantive foreign monetary support | Immediate | Washington Regional Counterintelligence Office (WRCO) |
| | All unofficial travel to sensitive country | 30+ days prior to departure, and after return | Washington Regional Counterintelligence Office (WRCO) |



**Insider Threat:**
An insider threat is when an employee decides to commit espionage and takes the initiative to establish contact with a foreign intelligence service.

**Countering the Threat:**

- Integrate CI awareness into everyday work and observations.
- Understand that the threat is real and impacts everyone within DOE; it does not matter whether you have a clearance or not.
- Report CI concerns to your local CI Office immediately.

**Contact Your Washington Regional Counterintelligence Office if:**

- You are a DOE official business traveler or host of a foreign visitor in order to receive the required briefings and debriefings.
- You receive requests for access or information beyond normal requests.
- You observe an unexplained knowledge of DOE programs or personnel by foreign nationals.

**Your CI Office Contacts:**
Germantown—301-903-0467
Forrestal—202-586-8751

# THE OFFICE OF CLASSIFICATION

Classification is the act or process by which information is determined to be classified information. Proper protection of classified matter cannot be provided if a correct classification determination has not been accomplished.

The legal authority for classification is provided by statutes enacted by the Congress, such as the Atomic Energy Act of 1954, and Executive Orders issued by the President of the United States. These statutes and Executive Orders also provide stringent limits on what may or may not be classified and by whom.

Any person who originates documents is responsible for ensuring that they are properly classified. If that person lacks authority to classify, they must submit the documents to an authorized classifier for a classification determination. You will find more information on classification authorities and guidance later in this Handbook.

Success of the Department's Classification Program depends upon everyone being aware of their personal responsibilities for ensuring proper classification. If you have questions concerning classification, contact your organization's HSO, Classification Representative, or the Office of Classification.

# HEADQUARTERS SECURITY PROCEDURES

### HEADQUARTERS FACILITIES MASTER SECURITY PLAN (HQFMSP)

This Plan implements existing DOE security policies and procedures for all Headquarters facilities and Headquarters Elements. The Plan provides an overview of Departmental security policies and procedures and describes the organization designed to protect the property and national security interests of the Headquarters complex in the Washington, D.C. metropolitan area. Your HSO has a copy of this Plan, including an Appendix to the Plan that contains information unique to your organization. Contact your HSO to obtain a copy of the HQFMSP.

### PROHIBITED ARTICLES

A sign identifying prohibited articles is posted at the entrances to all Headquarters buildings. In short, weapons, explosives, or other dangerous instruments or materials that can injure people or damage the property are prohibited. Other prohibited items include alcoholic beverages and controlled substances (e.g., illegal drugs or paraphernalia, but not prescription medication.)

### CONTROLLED ARTICLES

- Controlled articles are not permitted in Limited or Exclusion Security Areas. These areas have been



### Reporting Requirements

| WHO | WHAT | WHEN | WHERE |
|---|---|---|---|
| All individuals | Lost, stolen or misused DOE badge | Within 24 hours | Forrestal or Germantown Badging Office or Office of Headquarters Security Operations |
| | Incidents of safeguards and security concern including those involving classified information/ matter or Special Nuclear Material (SNM) | Immediate | Office of Headquarters Security Operations or HSO |
| | Non-criminal violations relating to DOE programs like waste or abuse | Immediate | Your supervisor or Office of Inspector General or General Counsel |
| | Criminal violations relating to DOE programs like fraud | Immediate | Office of Inspector General Hotline 1-800-541-1625 |
| | Deliberate compromise or foreign involvement in suspected compromise of classified information | Immediate | Washington Regional Counterintelligence Office (WRCO) |

*NOTE. Always store classified waste in security containers, or in vaults or vault¯type rooms approved for classified open storage.*

Contact your HSO or consult the HQFMSP for additional information regarding collection locations, destruction witnessing requirements, records of destruction, etc.

**Cover Sheets**
Classified Document Cover Sheets serve as shields to protect Top Secret, Secret and Confidential documents from inadvertent disclosure. Always place a cover sheet on the face of each classified document when it is in use or removed from a security container. Cover sheets are required on the back of a classified document if the back page is not stamped with the overall highest classification level of the document.

**Cyber Security**
The Headquarters Cyber Security Program for classified and unclassified computer security is managed by the Office of the Chief Information Officer (IM). Classified matter may not be processed on Information Systems until the system is approved for classified use by the IM. Contact your HSO or ISSO for additional information.

**Reporting Requirements**
Incidents of security concern are events which are of concern to the DOE Safeguards and Security Program that warrant preliminary inquiry and subsequent reporting. As such, incidents of security concern, as well as information bearing on a Federal or contractor employee's continued eligibility for access to DOE facilities, material, or classified information must be reported to DOE Officials.

The nature of the reportable information will determine which office it should be reported to and the reporting deadlines. Below is the current list of safeguards and security reporting requirements for and about individuals. You are required to adhere to all reporting requirements that are applicable to you.



established to protect classified matter and other DOE security interests. (See additional Security Area discussion below.) Signs are posted at the entrances listing the articles which are prohibited from being introduced into these areas. Examples of Controlled Articles include:

- Cellular telephones with video recording capability.
- Electronic equipment, including toys, with an audio, video, optical, data recording or radio frequency transmitting or carrier current capability.
- Electronic equipment with a data exchange port capable of being connected to automated information system equipment.
- Personally owned computers and associated media.
- Cameras (film and electronic).

Prohibited articles listed above are also excluded from Limited or Exclusion Security Areas.

**VISITOR ESCORT REQUIREMENTS**
During normal operating hours, 6:00 a.m. to 8:30 p.m. Monday through Friday, escorts are not required for visitors entering Headquarters facilities unless specified by the office or person being visited. However, uncleared visitors must be escorted at all times and all days in Security Areas. The sponsoring office or person being visited is responsible for providing an escort, if required.

When escorting visitors, escorts must be with the visitor at all times. If escort responsibilities are delegated to another person, that person must be made aware of their escort responsibilities. Escorts must ensure that the visitor(s):

- Is not afforded unauthorized access to classified matter or posted Security Areas.
- Wears his or her Headquarters visitor badge above the waist, in a clearly visible manner at all times.
- Does not introduce any prohibited or controlled articles into the facility or Security Area, as applicable.
- Does not remove Government property from the facility except in accordance with established property accountability procedures.
- Complies fully with all Headquarters security requirements.

## SECURITY BADGES

Headquarters issues photo identification security badges to DOE Federal and contractor employees who require long-term routine access to the Headquarters buildings. These badges identify the individual and contain an Access Authorization indicator ("Q" or "L") for those individuals who have been granted a DOE access authorization. Individuals who require long term access to the HQ buildings but do not require access to classified matter are issued Building Access Only (BAO) badges. Headquarters also issues temporary badges, without photos, to visitors and employees who have lost or forgotten their badge.

In Headquarters buildings, employees and visitors must wear their badge above the waist, in plain view, with the photo showing. Employees should also remove their badge when outside the building. Security badges are not to be used for unofficial purposes such as cashing checks. Employees should notify the Headquarters badging office to obtain a new badge if they officially change their name, have a significant change in facial appearance or have a damaged badge.

NOTE: *Immediately notify the badging office if your badge is ever lost or stolen.*

Forrestal Badging Office
202-586-5764
Germantown Badging Office
301-903-3330

**BAO Badge**


## INSPECTIONS

All hand-carried articles are subject to inspection by Security Officers upon entry into or exit from a Headquarters facility. Other inspections may be conducted of any employee, contractor or visitor and their hand-carried items, with probable cause, within the Headquarters facilities as directed by the Office of Headquarters Security Operations. Headquarters uses a random inspection process and various explosive detection methods to detect and deter vehicle-transported explosive devices.



made to destroy classified matter, the actual destruction requires additional considerations. For example:

**Classified Paper Products**. Classified matter must always be destroyed beyond recognition to prevent reconstruction. Classified paper waste must be reduced to particulate of not more than **1/32" x 1/2"** during the destruction process. (**Note**: Newer particulate standards of 1mm x 5mm are required as current equipment is replaced or new equipment procured.) Headquarters uses approved shredders or the Classified Destruction Facility at Germantown to destroy classified matter and unclassified controlled information paper products. Contact your HSO for the locations of your organization's approved shredders as well as specific destruction procedures. All shredders approved for the destruction of classified matter are designated by conspicuously posted signs containing the make and model of the shredder and are signed by the approving HSO.

**Classified Tapes, Diskettes, and Cassettes.** Video tapes, viewgraphs, audio tapes, and similar magnetic media must be destroyed at the Germantown Classified Destruction Facility. Contact your HSO for additional information.

**Preparing Classified Matter for Destruction.** Paper, plastics, and metallic computer discs must be sorted into separate, properly annotated burn bags. Be sure to remove paper clips, staples, and metal or plastic fasteners from all documents. The name, routing symbol, telephone number, and room number of the person responsible for the bag must be clearly marked on the side of each bag for identification. Red-stripe bags are available in the self-service supply rooms.

Classified waste must be placed in red-striped burn bags and unclassified controlled information must be placed in plain brown bags prior to transport to the Germantown Classified Destruction Facility.

**Electronic Mail (E-Mail)**
Classified e-mail messages may be transmitted only on systems approved for classified transmissions and in accordance with an approved security plan. Consult your HSO or your Information Systems Security Officer (ISSO) for additional information.

**Transmitting Top Secret Matter**
Top Secret matter may be transmitted by the Defense Courier Service or the Department of State Courier System. Top Secret matter may be transmitted over approved secure communications networks. Individuals may be authorized to hand-carry Top Secret matter. No Top Secret matter may be transmitted without the express case-by-case approval of an organization's HSO, coordination with organizational CDC Station personnel, and completion of a Hand Carry Briefing. Consult your HSO for additional guidance.

**Reproducing Classified Documents**
Reproduction of classified documents shall be limited to the minimum number of copies consistent with operational requirements and further reproduction limitations indicated on the document. Only appropriately cleared individuals are authorized to reproduce classified matter. Reproduced copies are subject to the same protection and control requirements as the original document.

Reproduction of classified documents must be performed on machines located only within Limited or Exclusion Security Areas and specifically approved for classified reproduction. In accordance with the HQFMSP, HSO approval is required to deviate from these requirements on a case-by-case basis. Authorized machines are designated by conspicuously posted copier certification signs specifying up to the highest level and category of information that may be reproduced. Contact your HSO or consult the HQFMSP for additional information.

**DESTROYING CLASSIFIED MATTER**
Multiple copies, obsolete documents, and classified waste must be destroyed when no longer required. When the decision is



**SECURITY AREAS**
Headquarters Program Offices have established Limited and Exclusion Security Areas to protect classified matter. These areas have clearly defined boundaries and access control points. Access to Security Areas is limited to appropriately cleared and authorized individuals. All uncleared individuals requiring access to these areas must be escorted by a cleared and knowledgeable individual. In some security areas, sign-in registers are required. Similar to prohibited articles, certain controlled items are not permitted in Security Areas.

Contact your HSO if you have questions about the Security Areas established for your organization. If you have any questions about prohibited and controlled articles, contact your HSO or the Headquarters Physical Protection Team at 202-586-8075.

**CLASSIFIED REPOSITORIES AND STORAGE**
At Headquarters, classified repositories include GSA-approved security containers and approved vaults and vault-type rooms. Unless an area (e.g., vault or vault-type room) is approved for classified open storage, classified matter MUST always be stored in GSA-approved security containers located in approved Limited or Exclusion Security Areas. All GSA-approved security containers are equipped with XO series electromechanical combination locks.

All security areas approved for classified storage are posted with conspicuous signs indicating the maximum classification level and category authorized to be stored in the area. The sign will also state whether the area is approved for open or closed classified storage. The storage of classified matter within a GSA-approved security container is termed closed storage. The storage of classified matter within a secure storage repository (e.g., vault, vault-type room) in a manner such that a person could view the material if he/she has access to the room is termed open storage. At Headquarters, filing cabinets are NOT approved for classified storage unless they are used in an approved open storage vault or vault-type room.

**Combinations to Classified Repositories**
Always protect security container combinations at the classification level and category of the information contained in the container. Combinations must be changed whenever personnel knowing the combination transfer, terminate employment, when their access authorization is downgraded or terminated, or when the combination is known or suspected to have been compromised. Additional requirements apply for combinations to repositories (e.g., GSA-approved safes used to store NATO information).

*NOTE. Only an appropriately cleared and authorized individual may change container combinations.*

The Standard Form (SF) 700, "Security Container Information," must be used to record security container combinations and the SF 700 must be protected as classified matter. Consult the HQFMSP for additional information on the proper use and handling of the SF 700 and protecting and storing combinations to classified repositories.

**Recording Repository Openings and Closings**
An integral part of the Headquarters security check system involves use of the SF 702, "Security Container Check Sheet." This form records the times, dates, and the initials of individuals who have opened, closed, or checked a particular container, room, or vault. At Headquarters, the SF 702 must be affixed to security containers or entrances to Security Areas, vaults and vault-type rooms. However, the form is not required for card reader-controlled Limited Security areas with video surveillance integrated into the Central Alarm Station (CAS) or on Limited Area doors fully alarmed to the CAS. Limited Area doors internal to these types of areas are not required to have an SF 702 posted.

**Area Security Checks**
The SF 701, "Activity Security Checklist," provides a systematic means of recording the checking of end-of-day activities for a particular work area approved for classified



contractor employees must be authorized by the individual's organization to hand carry classified matter and authorization may be granted if the individual has received a "Hand Carry Security Briefing". Hand carrying classified matter aboard a commercial aircraft requires case-by-case approval by your Element and a special security briefing. Contact your HSO for additional information.

**U.S. Postal Service**
Secret and Confidential documents transmitted through the U.S. Postal Service (USPS) must be double-wrapped as described above. Only REGISTERED mail is authorized for Secret matter. Either REGISTERED or CERTIFIED mail is authorized for Confidential matter. Top Secret matter may not be transmitted via USPS.

**Commercial Express Delivery Services**
Transmitting Secret or Confidential matter by express services is only authorized when there is an urgent need for the information at the receiving facility on the next working day and no other approved method of transmission (e.g., secure facsimile) is available. As a general rule, this service may not be used on a Friday or the day preceding a holiday. Federal Express is the only Headquarters-approved commercial express company. Top Secret matter may not be transmitted by any express service. Check with your CDC Station personnel or your HSO for additional information.

**Secure Facsimile Equipment**
Sending classified information over unsecure or unencrypted office facsimile machines is strictly prohibited. Secure encrypted facsimile (FAX) machines are located in the Forrestal and Germantown Message Centers as well as other Headquarters Limited and Exclusion Security Areas. Secure facsimile machines authorized for processing classified information must be accredited and provide protection as classified computers and must operate through STU-III/STE encryption devices. Contact your CDC Station personnel or your HSO for additional information.

(if RD or FRD). The outer envelope or wrapper must be addressed with the CMA for both the sender and addressee, with no indication of the classification or category of the contents. Each Headquarters organization has Classified Control Station Personnel responsible for controlling classified matter transmitted outside the Element. Consult your HSO or CDC Station personnel for additional information.

**Hand Carrying Classified Matter**
Classified matter transmitted between Headquarters facilities (e.g., the Forrestal and Germantown buildings) must be properly prepared by CDC Station personnel including double-wrapping, use of CMA addresses, classification markings, receipts, etc. A locked briefcase tagged with the CMA may substitute for the outer-wrapping for a locally hand carried item. If hand carrying outside the D.C. Metropolitan Area, a locked briefcase may NOT substitute for the outer wrapping. A manifest signed by the hand carrier listing all hand carried material must be left with your organization's assigned CDC personnel each time you hand carry classified material outside a Headquarters building. You must also carry a copy of the manifest with you while hand carrying. A classified Receipt may be used as the manifest.

Classified documents carried between Security Areas in the same Headquarters building may be transported in a HQ Form 1410.5 "Candy-Stripe" envelope. The Candy-Stripe envelope serves as the outer wrapper. No inner wrapper is required, but the document must have the appropriate cover sheet attached. Contact your HSO for guidance if a Candy-Stripe envelope is not available.

The Department discourages hand carrying of classified documents. Transmitting classified matter through other approved channels (e.g., classified facsimile, FedEx, etc.) may be more efficient. If you do hand carry classified matter, keep the matter continuously in your possession until stored in an approved security repository. Additionally, classified matter may not be removed to private residences or other unapproved places such as restaurants or hotel rooms. All Federal and



operations. Headquarters requires the use of the SF 701, or an equivalent, for end-of-day Security Area inspections. Contact your HSO for additional information about the use of security checklists in your area.

**TELEPHONE CONVERSATIONS**
Classified information must never be discussed over unencrypted or unsecured telephone systems. Attempts to talk around classified information by using personally devised code words, nicknames, or paraphrasing is prohibited.

When using telephones approved for classified discussions [i.e., a Secure Telephone Unit (STU)-III or Secure Telephone Equipment (STE)]:

- You are responsible for ensuring the person on the distant end possesses the appropriate access authorization and need-to-know.
- You are also responsible for ensuring that the classified portion of the conversation is not overheard by uncleared personnel in your office area. Most offices are not soundproof, and voices tend to carry into adjacent offices and hallways. Always check adjacent hallways and offices for uncleared persons, or for persons without a "need-to-know".
- STU-IIIs and STEs must be located in a Limited or Exclusion Security Area.

**CLASSIFIED CONFERENCES AND DISCUSSIONS**
As a general rule, classified discussions, conversations, or conferences must be held in formally established and approved Limited and Exclusion Security Areas. Hosts of classified conferences or parties to classified discussions must take certain precautions to ensure that classified information is not compromised. These precautions include:

- Determining before the conference or discussion that all participants have been positively identified, have proper access authorization, and are otherwise authorized access to the information.
- Informing participants of Security Area controlled article requirements.

- Notifying participants of the classification level and category, if RD or FRD, of the information being discussed.
- Notifying participants that notes (handwritten or electronic) must be turned in to the host for classification review.
- Using only approved secure telephone equipment, (i.e., a STU‑III or STE) for classified telephone conversations.
- Ensuring the office or room door is CLOSED.

NOTE: *Classified discussions, meetings, or conferences held outside approved Security Areas require specific case-by-case approvals. Contact your HSO for additional information.*

**FOREIGN TRAVEL**

All **official** foreign travel requests must be entered into the Foreign Travel Management System (FTMS) within 30 calendar days before the proposed departure date, or 45 calendar days before the proposed departure date, if the travel is to a sensitive country or involves a sensitive subject. This requirement applies to both cleared and uncleared Federal and contractor employees. FTMS will issue notification of foreign travel to the appropriate security officials (i.e., Intelligence Directorate, Counterintelligence Directorate, HSO, etc.) to ensure review for compliance with U.S. and DOE official security policies and guidance. Contact your HSO or consult the HQFMSP to obtain additional information including the lists of sensitive countries and sensitive subjects.

Federal employees are required to report all unofficial travel to sensitive countries to the Counterintelligence Directorate 30 days prior to departure.

**BOMB THREATS**

Most bomb threats are conveyed by telephone. Employees should become familiar with procedures that deal with malicious or threatening telephone calls and with the telephone bomb threat checklist located in the back of the DOE National Telephone Directory.



- Completed parts 2 and 2A of the SF 700, Security Container Information, for a container is an accountable document if any of the information stored in that container is accountable. It does not, however, need to be placed into the formal accountability system; it must be accounted for according to local written procedures.

Each Headquarters organization has assigned Classified Document Control (CDC) Station personnel responsible for the receipt of all classified mail and controlling/preparing classified matter to be transmitted outside the organization.

Contact your HSO or consult the HQFMSP for additional information.

**Transmitting Classified Matter**

Before transmitting a classified document, the sender must ensure the recipient needs the information in the performance of their official duties (need-to-know), is authorized to receive the information (possesses the appropriate clearance), has an approved Classified Mailing Address (CMA), and has approved storage facilities for protecting the information. The CMA must be verified by consulting the Safeguards and Security Information Management System (SSIMS) database. All facilities authorized for the receipt of classified matter from Headquarters must be recorded in SSIMS before transmitting the classified matter. All classified matter must be double-wrapped before being transmitted outside a facility. The inner envelope or wrapper must be properly addressed with the CMA for both the sender and addressee, and bear the appropriate classification (Top Secret, Secret or Confidential) and category

- Secret matter stored outside a Limited Area (LA) (or higher). (Note: HQ does not allow Secret to be stored outside a LA or higher.)

- Any matter that requires accountability because of national, international, or programmatic requirements such as the following:

  classified computer equipment and media supporting the Nuclear Emergency Support Team (NEST) and Accident Response Group (ARG) operations and similar elements;

  national requirements such as cryptography and designated COMSEC;

  international requirements such as NATO ATOMAL, designated United Kingdom documents, or other FGI designated in international agreements; and

  special programmatic requirements (e.g., designated SAPs and Sigma 14).

- Classified Removable Electronic Media (CREM) which is required to be marked as S/RD or higher classification, or which contain Sigma 1, Sigma 2, Sigma 14, or Sigma 15 or a combination of nuclear weapons design/testing data. This matter is designated accountable classified removable electronic media, or ACREM. Specific rigorous storage, inventory, custodial, and handling requirements apply to ACREM and are covered in separate ACREM training.



Immediately report any written, verbal, or visual evidence of a suspected bomb or bomb threat to the Protective Force on telephone extension 166 at either the Forrestal or Germantown facility. The telephone numbers for reporting may be different if you work in a Headquarters building outside of the Forrestal or Germantown facilities. Contact your HSO or consult the HQFMSP for additional information.

**SECURITY INFRACTIONS**

- A Security Infraction is any knowing, willful, or negligent action contrary to the requirements of Executive Order 12958, *Classified National Security Information*, as amended, or its implementing directive that does not constitute a "violation."

Committing a security infraction may result in administrative discipline, including loss of access authorization. The incidents listed below may be considered security infractions. Note that this list is not all-inclusive. If security personnel find these actions were intentional or caused by gross negligence, the action may constitute a "violation", resulting in criminal prosecution or other administrative action.

- Leaving classified documents or material exposed and unattended or unsecured, to include leaving a classified repository open and unattended.
- Failure to properly safeguard classified documents or combinations to repositories.
- Changing a document's classification marking without proper authority.
- Destruction of classified documents in other than the prescribed manner.
- Improper transmission of classified documents or material.
- Failure to report known or suspected incidents of security concern.
- Failure to escort uncleared persons within Security Areas.
- Failure to comply with Cyber Security Policy.

- Unauthorized possession of prohibited articles in Headquarters facilities.

Contact your HSO or consult the HQFMSP for additional information.

**SECURITY VIOLATIONS**
Any action or intent that constitutes a violation of U.S. law or Executive Order or the implementing directives. Suspected or known violations of U.S. criminal statutes, federal statues, or federal laws pertaining to the unauthorized disclosure of classified matter are referred to federal law enforcement for further action.

# CLASSIFIED MATTER PROTECTION AND CONTROL

**TYPES OF INFORMATION**
The Department originates and receives unclassified, unclassified controlled information and classified information/ matter. Each type will be further discussed below, but the main emphasis of this Handbook is directed toward the protection of classified information.

**UNCLASSIFIED INFORMATION**
Information that is not classified and does not cause damage to the national security when disclosed is unclassified. A document may be marked to show that it is "unclassified" if it is essential to convey to any person who has access to the document that it is not classified. However, in most cases, unclassified markings are not applied when an entire document is unclassified. **NOTE:** *The fact that a document is unclassified does not mean it is publicly releasable*.

**UNCLASSIFIED CONTROLLED INFORMATION**
Unclassified Controlled Information is unclassified information that may be exempt from public release under the Freedom of Information Act. Some examples of



All employees making an oral presentation in a subject area that may be classified must submit the proposed text to their Classification Officer for classification review prior to making the presentation.

The originator of the document is responsible for submitting the document for classification review and subsequently for ensuring that it is properly marked. Until the document that may contain classified has been reviewed, it must be protected as classified, and access must be limited to authorized, cleared individuals. Contact your HSO or consult the HQFMSP for additional information.

**Declassification**
A Derivative Declassifier may derivatively declassify a document or material originated in only those organizations and subject areas for which he/she has been delegated such authority and is governed by other limitations specified in the written designation. A Derivative Declassifier shall base his/ her determinations on classification guidance pertaining to the specific subject areas described in the declassifier's designation of authority. Contact your HSO for additional information.

**Classified Document Control Stations and Accountability**

Classified Document Control (CDC) Stations are established and used to prevent unauthorized access to or removal of classified information. Accountability systems provide a system of procedures that provide an audit trail. Accountability applies regardless of the physical form of the matter (e.g., electronic, paper, or parts).

Accountable Matter. The following are types of accountable matter.

- Top Secret matter.

Classifiers must meet certain eligibility requirements and successfully complete classification training before they are authorized to formally classify documents. Contact your HSO for additional information.

**Classification**
Original classification authority is the authority to classify information as National Security Information (NSI). An Original Classifier makes the initial determination that information requires protection against unauthorized disclosure in the interest of national security. A Derivative Classifier is an individual authorized to determine that material is unclassified or classified (RD, FRD or NSI) in accordance with source documents. A Derivative Classifier makes the determination that documents or material contain or reveal information classified in accordance with classification guides, source documents, or instructions from an original classifier.

Under the Atomic Energy Act of 1954, RD is classified and remains so until formally declassified by DOE. FRD is transclassified from the RD category by joint determination of DOE and DOD and remains classified until jointly declassified by these agencies. All classification decisions concerning RD or FRD are derivative classification determinations.

Anyone who originates a document or material in a subject area that may be classified must submit the document to an authorized classifier for a classification review prior to distribution.

A document or material that is prepared in a potentially classified subject area that is intended for public release or widespread distribution must also be submitted to the organization's Classification Officer for classification review prior to distribution.



Unclassified Controlled Information subject to special handling restrictions include:

- **Other-Agency Controlled Information.**
  Unclassified Controlled Information created by other agencies. Examples include State Department information known as "Sensitive But Unclassified" (SBU) and Department of Defense information known as "For Official Use Only" (FOUO). Protection requirements for this type of information are established by the originating agency.

- **Official Use Only (OUO).**
  OUO is unclassified information that has not been given a classification pursuant to the criteria of a statute or Executive Order but that may be withheld from public disclosure under the criteria of the Freedom of Information Act (FOIA). OUO documents must be:
  - Properly marked to include a FOIA exemption category.
  - Be distributed only to individuals who need the information in the conduct of official business.
  - Stored to preclude disclosure.
  - Properly transmitted and properly destroyed.

  Contact your HSO or consult the HQFMSP to obtain additional information.

- **Unclassified Controlled Nuclear Information (UCNI).**
  UCNI is unclassified but sensitive information concerning nuclear material, weapons, and components the distribution of which is controlled under Section 148 of the Atomic Energy Act. UCNI must be stored in a locked drawer, locked desk, locked repository or a key-locked room when not in use. Contact your HSO or consult the HQFMSP to obtain additional information.

  NOTE. Remember that OUO, UCNI, and similar markings are protective markings and not classification markings.

## CLASSIFIED INFORMATION

What is classified information? Classified information is information or material that has been determined, pursuant to Executive Order 12958 or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure. Classified information includes Restricted Data (RD), Formerly Restricted Data (FRD) and National Security Information (NSI). The potential damage to national security for each is denoted by the classification levels of Top Secret, Secret or Confidential.

### Classification Levels

All classified information falls within one of three classification levels: Top Secret (TS), Secret (S), and Confidential (C). The significance of these levels, which reflects the varying degrees of sensitivity, is described as follows:

- **TOP SECRET.** The classification level assigned to information of utmost importance to the national defense and security. Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.

- **SECRET**. The classification level applied to information for which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.

- **CONFIDENTIAL.** The classification level applied to information for which the unauthorized disclosure could reasonably be expected to cause damage to national security.

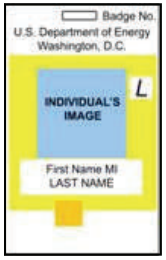
### Classification Categories

All classified information falls within one of three classification categories: Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).



| Access Authorization | Restricted Data (RD) | Formerly Restricted Data (FRD) | National Security Information (NSI) |
|---|---|---|---|
| "Q" | Top Secret<br>Secret<br>Confidential | Top Secret<br>Secret<br>Confidential | Top Secret<br>Secret<br>Confidential |
| "L" | ---<br>---<br>Confidential | ---<br>Secret<br>Confidential | ---<br>Secret<br>Confidential |

"Q" and "L" Access Authorization Indicators are visible on Federal and contractor security badges. See the discussion below for additional information on DOE security badges.


### Marking Classified Documents

Classified matter, regardless of date or agency of origin, must be marked to show the classification level, the classification category (if RD or FRD), special markings or caveats, classifier and originator identification and the date of origin. Additionally, titles or subjects of classified documents containing classified information must be portion marked. Unclassified Controlled Nuclear Information (UCNI) documents also require specific markings as specified in related DOE directives. Contact your HSO or consult the HQFMSP for additional information.

### Classification/Declassification Authority

The Department grants classification/declassification authority to specific individuals in specific positions for a specified time period. There are two basic types of classification authority: Original and Derivative. Original Classifiers and Derivative

## ACCESS TO CLASSIFIED INFORMATION

Access to classified information is granted only to persons who possess the appropriate access authorization and who require access in the performance of official or contractual duties (need-to-know). If you disseminate classified matter, you must ensure the recipient has the appropriate security clearance and need-to-know. What is need-to-know?

**Need-to-Know**.

Need-to-know is a determination made by an authorized holder of classified or unclassified controlled information that a prospective recipient requires access to the specific classified or unclassified controlled information in order to perform or assist in a lawful and authorized Governmental function. All employees have the duty to adhere to the "need-to-know" policy as part of their personal security responsibilities. Check with your supervisor if there is any doubt in your mind as to an individual's "need-to-know".

No person may have access to classified information unless he or she has been granted an access authorization equal to, or higher than, the classification level and category of the information, and the requisite "need-to-know". Additionally, no person is entitled to access classified information solely by virtue of their rank, office, position, or security clearance.

**Access Authorizations.**

An Access Authorization is an administrative determination that an individual is eligible for access to classified matter when required by official duties or is eligible for access to, or control over, special nuclear material. The Department issues "Q" and "L" access authorizations. Each access authorization ("Q" or "L") authorizes an individual to access specific levels and categories of classified information. The following table depicts the classification levels and categories of information that individuals possessing "Q" or "L" access authorizations are authorized to access:



- **RESTRICTED DATA (RD).** RD, defined in the Atomic Energy Act of 1954, is all data concerning the design, manufacture, or utilization of atomic weapons; the production of Special Nuclear Material; or the use of Special Nuclear Material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954.

- **FORMERLY RESTRICTED DATA (FRD).** Despite the term "Formerly," this information is classified information jointly determined by the DOE or its predecessors and the Department of Defense (DOD) to be related primarily to the military utilization of atomic weapons; removed from the RD category pursuant to Section 142(d) of the Atomic Energy Act, and protected as National Security Information subject to the restrictions of transmission to other countries and regional defense organizations that apply to RD.

- **NATIONAL SECURITY INFORMATION (NSI).** NSI is any information that has been determined, pursuant to Executive Order 12958 or any predecessor Order, to require protection against unauthorized disclosure and that is so designated. NSI does not include RD or FRD.

## SPECIAL MARKINGS AND HANDLING CAVEATS

Special markings and caveat markings are placed on documents either to describe special handling or dissemination requirements or to identify the type of information and the originator. In some cases, access to the documents may require approval of special program offices or managers. The following are examples of some of the most commonly used caveats:

**Foreign Government Information (FGI).**

- Information that is provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

- Information that is produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
- Information that is received and treated as "Foreign Government Information" under the terms of Executive Order 12958, *Classified National Security Information*, as amended or a predecessor order.

**North Atlantic Treaty Organization (NATO) Information.**
The following markings are used for classified NATO material:

- NATO material has four levels of classified information: **COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR)**. When NATO or COSMIC precedes a classification, the information is the property of NATO. Additional rules apply.

- The **ATOMAL** marking is a NATO marking that is applied to RD or FRD provided by the United States to NATO, or to United Kingdom Atomic Information provided by the United Kingdom. ATOMAL information is classified either as COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA), depending on the damage that would result from unauthorized disclosure.

**Director of Central Intelligence Information**.
The following are markings authorized for Intelligence Information:

- **No Foreign Dissemination (NOFORN).** This marking indicates that the information contained in the document must not be released to foreign governments, international organizations, coalition partners, foreign nationals or immigrant aliens without originator approval.



- **Originator Controlled (ORCON).** This marking indicates that the document bearing the marking is controlled by the originator. Reproduction, extraction of information, or redistribution of such documents requires the permission of the originator.

- **Proprietary Information (PROPIN).** This marking indicates that the information contained in the document must not be released outside the government in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information, without the permission of the originator of the intelligence and provider of the information.

- **Authorized for Release to Country (REL).** This marking applies to classified intelligence information that an originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to a specified foreign country(ies), or international organization(s).

**Weapon Data.**
The following are markings associated with atomic weapons or nuclear explosive devices.

- **Sigma Category.** This marking refers to Restricted Data and Formerly Restricted Data concerning the design, manufacture, storage, characteristics, performance effects, or use of nuclear weapons, nuclear weapon components, or nuclear explosive devices or materials.

- **Critical Nuclear Weapons Design Information (CNWDI).** A Department of Defense marking designating Top Secret or Secret Restricted Data weapons design information.